CLAIMS

1. A privacy management method, comprising:

first operations, effected by an owner of personal data, comprising:

encrypting that data based on encryption parameters comprising an encryption key string formed using at least policy data indicative of conditions, differing from recipient identity, to be satisfied before access is given to said personal data, and public data provided by a trusted party and related to private data of the latter,

providing the encrypted data to a recipient;

second operations, effected by the trusted party, comprising using the encryption key string and said private data to determine a decryption key, and outputting this key; at least one of these second operations only being effected after a further second operation has checked that said conditions are satisfied regarding said recipient.

2. A method according to claim 1, wherein the first operations further comprise providing the encryption key string to said recipient along with the encrypted data; the method further comprising intermediate operations in which the recipient provides the trusted party with the encryption key string and requests the decryption key.

3. A method according to claim 1, wherein the first operations further comprise providing details of the trusted party to said recipient along with the encrypted data.

4. A method according to any one of claims 1, further comprising said recipient sending on the encrypted personal data to a further party, and the trusted party providing the decryption key to that further party only after said conditions have been satisfied in respect of that further party.

5. A method according to claim 1, wherein in said first operations multiple items of personal data are encrypted each using said public data and a respective encryption key string formed using at least respective policy data; the encrypted multiple items being provided to said recipient; and wherein in the second operations the trusted party determines the decryption key for at least one encrypted item using the corresponding

encryption key string and said private data, the or each determined decryption key only being provided to said recipient after the conditions in the corresponding policy data have been satisfied.

6. A method according to claim 5, further comprising said recipient sending on a selected subset of said multiple encrypted items of personal data to a further party; and the trusted party providing to that further party a decryption key for an encrypted item provided to that party, only after the conditions in the corresponding policy data have been satisfied in respect of said further party.

7. A method according to claim 1, wherein the data owner has a set of policies that form respective nodes in a policy hierarchy, and wherein in said first operations, multiple items of personal data are encrypted and provided to said recipient, each such data item being independently associated with at least one node of the policy hierarchy and being encrypted using said public data and policy data formed by a concatenation of the policies of the nodes traversed between the root of the hierarchy and the said at least one node with which the data item is associated.

8. A method according to claim 1, wherein the data owner has a set of policies that form respective nodes in a policy hierarchy, and wherein in said first operations, multiple items of personal data are encrypted and provided to said recipient, each such data item being independently associated with at least one node of the policy hierarchy and being encrypted by an iterative process in which:

- the data item is encrypted using said public data and policy data formed by the policy of the said at least one associated node,
- the encrypted data thus produced then becoming a data item associated with the parent node of the or each node formed by the policy just used for encryption.

9. A method according to claim 1, wherein in said first operations, multiple items of personal data are encrypted and provided to said recipient, at least two of these data items being encrypted using public data of different respective trusted parties whereby the recipient must obtain the appropriate decryption key from a different one of the trusted parties in dependence on which data item the recipient wishes to access.

10. A method according to claim 1, wherein in said first operations an item of personal data is first encrypted using a first policy and the public data of a first trusted party with the encrypted data being then further encrypted using a second policy and the public data of a second trusted party whereby the recipient must obtain decryption keys from the two trusted parties in order to access the data item.

11. A method according to claim 1, wherein in said first operations the personal data is encrypted using public data provided by multiple trusted parties, the second operations being carried out by each of said multiple trusted parties to provide a respective decryption sub-key whereby to enable the recipient to decrypt the encrypted personal data by the combined use of the sub-keys from each trust authority; each trusted party ensuring that policy conditions for which it is competent have been satisfied before generating and/or outputting the corresponding sub-key.

12. A method according to claim 1, wherein the trusted party makes an audit record of each provision of a decryption key by the trusted party.

13. A method according to claim 12, wherein said audit record further comprises information about when a decryption key is not provided because a related policy condition has not been satisfied, this information including information about the condition failure.

14. A method according to claim 12, wherein the trusted party on receiving a request from a party for a decryption key in respect of a particular item of data, checks its audit records to ascertain whether the decryption key for that item has previously been provided to a different party, and if so, whether the policy associated with the data item permitted onward disclosure.

15. A method according to claim 14, wherein the trusted party, on determining that the decryption key for the data item was previously provided under a policy of no onward disclosure, refuses to provide the decryption key to the requesting party.

16. A method according to claim 1, wherein the first and second operations are repeated multiple times for the same or different personal data owned by the same or different personal-data owners and provided to the same or different recipients.

17. A method according to claim 16, wherein the trusted party makes an audit record of each provision of a decryption key by the trusted party.

18. A method according to claim 17, wherein said audit record comprises the identity of the personal data, personal-data owner and recipient concerned.

19. A method according to claim 17, wherein said audit record further comprises information about when a decryption key is not provided because a related policy condition has not been satisfied, this information including information about the condition failure.

20. A method according to claim 17, wherein the trusted party on receiving a request from a party for a decryption key in respect of a particular item of data, checks its audit records to ascertain whether the decryption key for that item has previously been provided to a different party, and if so, whether the policy associated with the data item permitted onward disclosure.

21. A method according to claim 20, wherein the trusted party, on determining that the decryption key for the data item was previously provided under a policy of no onward disclosure, refuses to provide the decryption key to the requesting party.

22. A method according to claim 1, wherein a said policy condition relates to the strength of cryptographic methods to be employed in authenticating the identity of the recipient before the decryption key is provided to the latter.

23. A method according to claim 1, wherein a said policy condition relates to the expiry date of the policy or of the personal data, the trusted party not providing the decryption key when the expiry date has passed.

24. A method according to claim 1, wherein a said policy condition relates to the trusted party communicating with the owner, the trusted party effecting this communication before providing the decryption key to said recipient.

25. A method according to claim 24, wherein the condition is that the trusted party obtain consent from the owner before providing the decryption key to said recipient.

26. A method according to claim 24, wherein contact details for the owner are contained in policy data in encrypted form, the contact details being encrypted using said public data of the trusted party and an encryption key string formed by a data element also included in the policy data whereby the trusted party can form the corresponding decryption key and decrypt the encrypted contact details.

27. A method according to claim 1, wherein a said policy condition relates to a computing platform being used by the recipient being a trusted platform running software of predetermined functionality that cannot be subverted.

28. A method according to claim 1, wherein the trusted party checks that any party requesting the decryption key is using a trusted computing platform running software of predetermined functionality that cannot be subverted.

29. A method according to claim 1, wherein the data owner, before providing the encrypted data to the recipient, checks that the latter is using a trusted computing platform running software of predetermined functionality that cannot be subverted.

30. A method according to claim 27, wherein the software being run by the computing entity of the recipient is arranged to prevent onward disclosure of data indicated in a predetermined manner, the data owner marking an item of personal data in this predetermined way before providing it to the recipient.

31. A method according to claim 1, wherein the data owner, before providing the encrypted data to the recipient, checks that the trust authority is using a trusted computing platform running software of predetermined functionality that cannot be subverted.

32. A method according to claim 1, wherein the recipient, before providing the trust authority with any data concerning itself for the purpose of satisfying a said condition, checks that the trusted party is using a trusted computing platform running software of predetermined functionality that cannot be subverted.

33. A method according to claim 1, wherein the recipient, before providing any personal data received from the data owner to another party, checks that the latter is using a trusted computing platform running software of predetermined functionality that cannot be subverted.

34. A method according to claim 1, wherein the owner of the personal data also serves as the trusted party.

35. A method according to claim 1, wherein said owner is acting as a proxy for a party to whom the personal data relates.

36. A method according to claim 1, wherein in the second operations the decryption key is not determined until after said conditions have been satisfied.

37. A privacy management system comprising first, second and third computing entities, wherein:

- the first computing entity comprises: a data store for holding personal data; an encryption unit for encrypting the personal data based on encryption parameters comprising both an encryption key string formed using at least policy data indicative of conditions, differing from recipient identity, to be satisfied before access is given to said personal data, and public data provided by the second computing entity and related to private data of the latter; and a communications interface for providing the encrypted data to the third computing entity;
- the second computing entity comprises a data store for holding said private data; a communications interface for receiving the encryption key string and for providing a corresponding decryption key to the third computing entity; a decryption-key determination unit for using the private data and the received encryption key string to

determine the corresponding decryption key for decrypting the encrypted data; and a condition-checking arrangement for ensuring that the decryption key is only determined, or only provided to the third computing entity, after the conditions in said policy data have been satisfied in respect of the third computing entity.

38. A system according to claim 37, wherein the first computing entity is arranged to provide the encryption key string to the third computing entity along with the encrypted data; the third computing entity being arranged to request the decryption key from the second computing entity and provide it with the encryption key string.

39. A system according to claim 37, further comprising a fourth computing entity, the third computing entity being arranged to send on the encrypted personal data to the fourth computing entity, and the second computing entity being arranged to provide the decryption key to the fourth computing entity only after said conditions have been satisfied in respect of that fourth computing entity.

40. A system according to claim 37, wherein the second computing entity is arranged to make an audit record of each provision of the decryption key by the second computing entity.

41. A system according to claim 40, wherein the second computing entity is arranged to include in the audit record, information about when a decryption key is not provided because a related policy condition has not been satisfied, this information including information about the condition failure.

42. A system according to claim 40, wherein the second computing entity is so arranged that upon receiving a request from a party for a decryption key in respect of a particular item of data, it checks its audit records to ascertain whether the decryption key for that item has previously been provided to a different party, and if so, whether the policy associated with the data item permitted onward disclosure.

43. A system according to claim 37, further comprising multiple first and third computing entities, the second computing entity being arranged to provide decryption keys for the

third computing entities in respect of personal data encrypted by the first computing entities provided the corresponding policy conditions have been satisfied in each case.

44. A system according to claim 37, wherein the second computing entity is arranged to make an audit record of each provision of a decryption key by the second computing entity.

45. A system according to claim 44, wherein said audit record comprises the identity of the first and third computing entities concerned with each provision of a decryption key.

46. A system according to claim 44, wherein the second computing entity is arranged to include in the audit record, information about when a decryption key is not provided because a related policy condition has not been satisfied, this information including information about the condition failure.

47. A system according to claim 44, wherein the second computing entity is so arranged that upon receiving a request from a party for a decryption key in respect of a particular item of data, it checks its audit records to ascertain whether the decryption key for that item has previously been provided to a different party, and if so, whether the policy associated with the data item permitted onward disclosure.

48. A system according to claim 37, wherein a said policy condition relates to the second computing entity communicating with the first computing, the second computing entity being arranged to effect this communication before providing the decryption key to said third computing entity.

49. A system according to claim 48, wherein the condition is that the second computing entity obtain consent from the first computing entity before providing the decryption key to the third computing entity.

50. A system according to claim 48, wherein contact details of the first computing entity are included in said policy data in encrypted form, the contact details being encrypted using said public data and an encryption key string formed by a data element also included

in the policy data whereby the second computing entity can form the corresponding decryption key and decrypt the encrypted contact details.

51. A system according to claim 37, wherein a said policy condition relates to the third computing entity being a trusted platform running software of predetermined functionality that cannot be subverted.

52. A system according to claim 37, wherein the first and second computing entities are combined.

53. A computing entity arranged to act as a trusted party, the computing entity comprising:

- a data store for holding private data;
- a communications interface for receiving an encryption key string and for outputting a corresponding decryption key to a requesting entity; the encryption key string being formed using at least policy data indicative of conditions, differing from recipient identity, to be satisfied before access is given to data encrypted with the key;
- a decryption-key determination unit for using the private data and a received encryption key string to determine a corresponding decryption key for decrypting data encrypted using the encryption key string and public data derived using said private data; and
- a condition-checking arrangement for ensuring that the decryption key is only determined, or only output via the communications interface, upon the conditions in said policy data being satisfied in respect of the requesting entity.

54. A computing entity according to claim 53, further comprising an audit-trail arrangement for making an audit record of each output of a decryption key to a requesting entity.

55. A computing entity according to claim 54, wherein the audit-trail arrangement is arranged to include in the audit record information about when a decryption key is not provided because a related policy condition has not been satisfied, this information including information about the condition failure.

56. A computing entity according to claim 54, in which the audit-trail arrangement is arranged, in response to the computing entity receiving a request from a party for a decryption key in respect of a particular item of data, to checks its audit records to ascertain whether the decryption key for that item has previously been provided to a different party, and if so, whether the policy associated with the data item permitted onward disclosure.

57. A computing entity according to claim 56, wherein the audit-trail arrangement is further arranged, on determining that the decryption key for the data item was previously provided under a policy of no onward disclosure, to block the generation and/or output of the decryption key.

58. A computing entity according to claim 53, wherein a said policy condition relates to the computing entity communicating with an owner of the encrypted data, the computing entity being arranged to effect this communication before generating and/or outputting the decryption key to the requesting entity.

59. A computing entity according to claim 58, wherein the condition is that the computing entity obtain consent from the owner of the encrypted data before providing the decryption key to the requesting entity.

60. A computing entity according to claim 53, wherein a said policy condition relates to the requesting entity being a trusted platform running software of predetermined functionality that cannot be subverted, the computing entity being arranged to communicate with the requesting entity to check this condition before generating and/or outputting the decryption key.